PATENT

C.   REMARKS

1.   Summary of the Claims

Claims 1, 3, 5, 7-8, 10-11, 13-14, 16, 18, and 20-27 are currently pending. Claims 1, 3, 5, 7-8, 10-11, 13-14, 16, 18, and 20-26 have been previously presented in the response filed April 21, 2005. Claim 27 is a new independent claim that has been added in this Supplemental Response. No claims have been amended or canceled in this Supplemental Response. Consideration and examination of new claim 27, and remarks thereto, is respectfully requested in addition to reconsideration of Applicants' amended claims and remarks thereto filed April 21, 2005.

2.   Claim Rejections

Rejections of claims 1, 3, 5, 7-8, 10-11, 13-14, 16, 18, and 20 as being anticipated under 35 U.S.C. § 102(e) by Gupta et al. (U.S. Patent No. 6,389,532, hereinafter "Gupta") and as being obvious, and therefore unpatentable, under 35 U.S.C. § 103(a) over Gupta in view of Goldstone (U.S. Publication No. 2002/0101819, hereinafter "Goldstone") and over Gupta in view of Klaus (U.S. Patent No. 5,892,903, hereinafter "Klaus") were previously traversed in Applicants' Response filed April 21, 2005. In this Supplemental Response, Applicants' focus on the patentability of new claim 27 over the cited references.

3. New Claim 27

Applicants have added new claim 27 which is directed to a method for "preventing malicious network attacks on a server computer from a client computer that accesses the server computer via a computer network" with limitations originally found in original claims 1, 3, 5, 6, and 7. Consequently, new claim 27 includes the limitations of:

- executing a test script that includes one or more attack simulations from the client computer, the execution of the test script including:

  o receiving, at the server computer, one or more packets from the client computer and one or more open socket requests from the client computer;

  o deciding a packet threshold for the client computer, the deciding including:

    ▪ determining a number of packets received from the client computer during a time interval;

    ▪ incrementing the number of packets received from the client computer; and

    ▪ comparing the number of packets received with a packet limit stored at the server computer;

  o computing an open socket threshold for the client computer, the computing including:

    ▪ determining a number of opened sockets for the client computer;

- incrementing the number of opened sockets for the client computer;

- comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and

o evaluating the packet limit and the socket limit used during the attack simulations, the evaluating including:

- analyzing the performance of the server computer during the simulation; and

- adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from a group consisting the stored packet limit and the stored socket limit.

Limitations of Applicants' original claims 3 and 5, which have been included new claim 27, were originally rejected using the Goldstone reference. In Applicants' Response filed April 21, 2005, Applicants filed a declaration, pursuant to 37 C.F.R. § 1.131, by Applicant Dwip Banerjee that removed the Goldstone reference as prior art. Therefore, Applicants respectfully submit that new claim 27 is allowable for at least the reason that Goldstone is not prior art and the limitations originally found in Applicants' claims 3 and 5 are allowable to the extent such limitations have been incorporated into claim 27.

Notwithstanding the allowability of claim 27 as described above, Applicants respectfully submit that the art of record

Docket No.   Page 14   Atty Ref. No. IBM-1020
AUS920010361US1
                    Banerjee et al. - 09/870,610

PATENT

simply does not teach or suggest the limitations set forth in claim 27 of *incrementing the number of packets received from the client computer.*

The Office Action contends that Goldstone teaches this limitation, and cites paragraph 0038 of Goldstone in support of this rejection. However, upon closer inspection, Goldstone does not teach or suggest *incrementing the number of packets received from the client*, as claimed by Applicants. Rather, Goldstone's paragraph 0038 states that:

> "…when a response is sent from the server to the client, acknowledging the intention to connect, the attacking client merely ignores the response, resulting in a half-open connection… The server under these circumstances, not realizing that there is no intention to connect, assumes that the request is legitimate and reserves buffer space for the connection…[and] the server's bandwidth will still get congested since the attacking client will continue to send bogus requests to the server." (emphasis added)

As can be seen, the Office Action reference discusses a server's bandwidth becoming congested because the server accepts bogus packet requests from a malicious client, and never teaches or suggests "incrementing the number of packets received" as claimed by Applicants.

The Examiner mentioned that it is inherent that a client increments the number of packets when Goldstone's client sends packets. Applicants, however, are not claiming the client incrementing the number of packets sent, but rather that the server is incrementing the number of packets received. Applicants claim 27 compare the number of packets received with a packet limit. The Office Action states that Gupta fails to teach the limitations in Applicants' claim 3, and

Docket No.   Page 15   Atty Ref. No. IBM-1020
AUS920010361US1
                    Banerjee et al. - 09/870,610

indeed Gupta does not.   Therefore, since neither Gupta nor Goldstone teach or suggest, in whole or in part, all the limitations included in Applicants' claim 27, claim 27 is allowable.

Limitations originally found in claim 7 have also been incorporated into claim 27. These limitations include:

- executing a test script, the test script including one or more attack simulations;

- determining whether to change one or more of the configuration settings based on the processing; and

- adjusting the configuration settings based on the determination.

The Office Action contends that Klaus teaches all the limitations included in Applicants' original claim 7, and cites column 9, lines 1-41 in Klaus in support of this rejection. However, upon closer inspection, Klaus does not teach or suggest "*determining whether to change one or more of the configuration settings based on the processing, and changing one or more of the configuration settings based on the determination*" as claimed by Applicants.   Rather, Klaus' reference states that:

> "...the system includes an IP spoofing attack generator 32, a source/destination address generator 34 and a service command generator 36.   Source/destination address generator 34 identifies the internet and physical addresses of the computers on the network 12 to be tested. Source/destination address generator 34 verifies that each computer on network 12 is emulated in IP spoofing attacks on all of the other computers on network 12.   In this manner, the inventive system exhaustibly tests all possible attack combinations on a network. Service command generator 36 generates commands for a service which may be coupled to a port which IP spoofing attack generator 32 is able to initiate a communications connection...   The service command received from command

Docket No.   Page 16   Atty Ref. No. IBM-1020
AUS920010361US1
                    Banerjee et al. - 09/870,610

message generator 36 and the source and destination addresses received from source/destination address generator 34 are used by IP spoofing attack generator 32 to provide data and header content for messages sent to transport layer 22 and network layer 24 of protocol stack 20 which are used to implement the IP spoofing attack and detection"

As can be seen, the Office Action reference discusses how Klaus tests a computer network for IP spoofing, but never teaches or suggests an <u>action</u> to take based on the results of the tests, let alone the limitations claimed by Applicants in claim 27 including:

- evaluating the packet limit and the server limit used during the attack simulations, the evaluating including:

  o analyzing the performance of the server computer during the simulation; and
  o adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from a group consisting the stored packet limit and the stored socket limit.

The Office Action admits that Gupta fails to teach the limitations in Applicants' claim 7 (now incorporated in claim 27), and indeed, upon review, Applicants agree that Gupta does not teach such limitations. Therefore, since neither Gupta nor Klaus teach or suggest, in whole or in part, all the limitations included in Applicants' original claim 7, as incorporated in new claim 27 is allowable.

Docket No.   Page 17   Atty Ref. No. IBM-1020
AUS920010361US1
                      Banerjee et al. - 09/870,610

Consequently, based on the foregoing, Applicants respectfully submit that new claim 27 is clearly patentable over the art of record. Accordingly, an *early allowance* of claim 27 is respectfully requested.

CONCLUSION

As a result of the foregoing, it is asserted by Applicants that new claim 27 added in this Supplemental Response is in condition for allowance, and Applicants respectfully request an early allowance of this claim.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By _____

Joseph T. Van Leeuwen
Attorney for Applicants
Registration No. 44,383
Telephone: (512) 301-6738
Facsimile: (512) 301-6742

Docket No.   Page 18   Atty Ref. No. IBM-1020
AUS920010361US1

Banerjee et al. - 09/870,610